

NAVAL WAR COLLEGE
Newport, R.I.

THE OPERATIONAL PROPONENT FOR INFORMATION WARFARE

by

Samuel R. Dick
Lieutenant Colonel, USAF

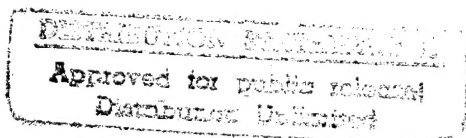
A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College, the Department of the Navy or the Department of the Air Force.

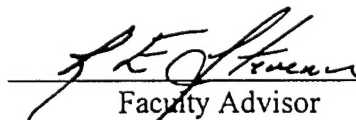
Signature: _____

14 June 1996

Paper directed by
Captain George W. Jackson, USN
Chairman, Joint Military Operations Department



DTIC QUALITY INSPECTION

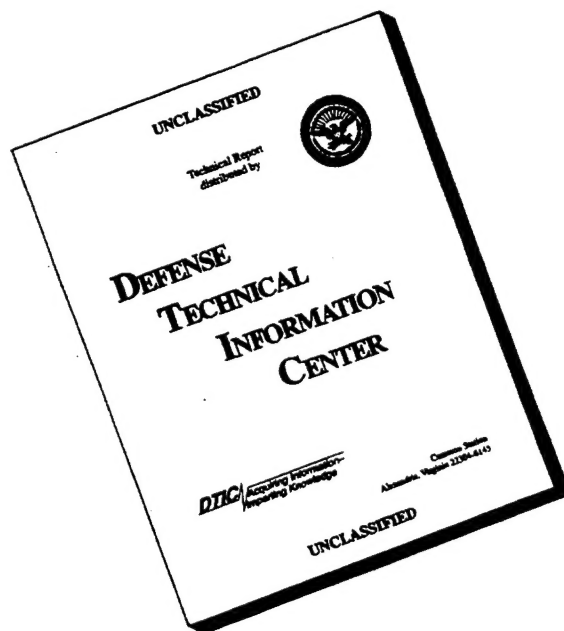

Faculty Advisor

15 MAY 96
Date

Commander Richard E. Stevens, USN
Jerry O. Tuttle Military Chair of
Command and Control Warfare

19960813 152

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

UNCLASSIFIED

Security Classification This Page

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): AN OPERATIONAL PROPONENT FOR INFORMATION WARFARE (U)			
9. Personal Authors: SAMEUL R. DICK, LT COL, US AIR FORCE			
10. Type of Report: FINAL		11. Date of Report: 16 MAY 96	
12. Page Count: 22			
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC, the US Air Force or the Department of the Navy.			
14. Ten key words that relate to your paper: INFORMATION WARFARE OPERATIONAL PROPONENT C2W JPOTF SPECIAL OPERATIONS ORGANIZATION WEAPONS			
15. Abstract: How Information Warfare is integrated into the Commander in Chief and Joint Task Force staffs will determine its successful application in wartime. Three criteria are formulated: 1) inter-agency participation, 2) national approval for operations, and 3) a long-term studies program. Three models are analyzed: 1) Command and Control Warfare cell, 2) Joint Psychological Operations Task Force, and 3) Special Operations Component. The most suitable choice using the three criteria is to establish an Information Warfare organization similar to the Joint Psychological Operations Task Force.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841- 655 6461		20. Office Symbol: C	

Security Classification of This Page Unclassified

TABLE OF CONTENTS

Title	Page
Title Page	i
Table of Contents	ii
List of Figures	iii
Abstract	iv
Introduction	1
Criteria	3
Inter-Agency	3
National Command Authorities	
Approval	4
Long-Term Studies	5
Three Models	6
C2W Cell Model	6
JPOTF Model	9
SOC Model	11
Conclusion	13
Endnotes	15
Bibliography	17

LIST OF FIGURES

<u>Figure</u>	<u>Title</u>	<u>Page</u>
Figure 1	Some Organizations Involved in Information Warfare	3
Figure 2	C2W Model	7
Figure 3	JPOTF Model	10
Figure 4	SOC Model	11

ABSTRACT

How Information Warfare is integrated into the Commander in Chief (CINC) and Joint Task Force (JTF) staffs will determine its successful application in wartime. Three criteria to estimate the success of an organization to use Information Warfare are formulated and applied to three possible models of theater organization to determine the most suitable choice.

The three criteria are 1) inter-agency participation, 2) national approval for operations, and 3) a long-term studies program.

The models range from subordinate planning cells, like the Command and Control Warfare cell, through component level task forces, like the Joint Psychological Operations Task Force (JPOTF), to an actual component commander, like the Special Operations Component.

The most suitable choice would be an organization like the JPOTF to coordinate and conduct Information Warfare for the CINCs and JTFs. The wide range of repercussions from this type of warfare, combined with the unique capabilities embedded in various agencies, the "one time" nature of some of these capabilities, and the need for detailed, long-term study to employ the capabilities, all support a structure similar to the component level JPOTF.

THE OPERATIONAL PROPONENT FOR INFORMATION WARFARE

INTRODUCTION

Information Warfare represents a growth industry for writers and thinkers of the military arts. Vigorous debates have raged in scholarly publications and at conferences about who should conduct Information Warfare and what it means to US security. Even the definition for what Information Warfare includes has been difficult to determine. With the printing of Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), an approved definition has been published:

[Information Warfare] is defined as actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.¹

Without much doubt, Information Warfare represents an important ingredient in how the US military will conduct future wars. To effectively employ this new arena of warfare will require a skillful blend of weapons, doctrine, and organization. With an effective balance of all three elements, the advances in information technologies can be realized as a revolution in military affairs. During World War I, for instance, the introduction of armored vehicles did not radically change the nature of that war. However, German adjustments to the use of armored vehicles by employing the doctrine of Blitzkrieg and organizing Panzer divisions did radically alter the nature of warfare during World War II. In the same way, Information Warfare weapons will not radically change warfare until these new weapons are honed and integrated into the US armed forces doctrine and organization. A critical part of this integration effort is the decision about how combat commanders and their staffs will organize to plan and execute Information Warfare. This discussion will focus on the decision at what is known as the operational level of war.

In US warfighting doctrine, the thinking about war is divided into primarily three levels. The strategic level of war refers to the use of the instruments of national power to achieve the highest scale objectives. The tactical level of war represents the lowest scale objectives, down to the actions of individual soldiers, sailors, and airmen. The operational level is the connection between the strategic and the tactical levels. This operational level of war is the primary province of the Combatant Commanders, also known as the Commanders in Chief (CINCs). The CINC's staff plans and directs actions within the theater or function the CINC is responsible for. The Joint Task Force (JTF) Commander is the CINC's primary subordinate for executing combat at the operational level. How the JTF's and CINC's staffs are formed to plan and execute Information Warfare, then, is the subject at hand when asked: "who should be the operational proponent for Information Warfare?"

To effectively judge who ought to fill the role of operational proponent for Information Warfare will require constructing an analytical framework to make comparisons. To build the framework, it is first necessary to understand the criteria the proponent must meet at the operational level. How well a proposed organization fulfills these criteria determines which organization should be chosen. Next, three current operational organizations faced with fulfilling similar challenging functions will be used as models. The first model is the staff planning cell, such as the C2W cell. The next model, the Joint Psychological Operations Task Force (JPOTF), serves primarily at the same level as a component commander, but has unique features that set it apart. Finally, the last model, the Special Operations Component (SOC), provides integration of forces as a full component. The ability of each of these models to meet the proponent criteria will be incorporated into describing their functions. Finally, one model will be recommended as a best fit to the criteria.

CRITERIA

Information Warfare requires an implementing organization that fulfills three diverse and sometimes competing criteria. First, the operational proponent must be an inter-agency organization. Also, the Information Warfare plans must be approved by the National Command Authorities or their designated representative. Finally, there must be a long term study program to provide the detailed information required to effectively plan and execute Information Warfare.

Inter-Agency. With the flurry of activity by many agencies to address Information Warfare, the tools of this kind of warfare have become spread throughout all of the individual services, various Department of Defense agencies, and agencies outside the Department of Defense. A sample of the diverse organizations with an impact on Information Warfare includes:

Joint Command and Control Warfare Center	Joint Chiefs of Staff
Air Force Information Warfare Center	Defense Information Systems Agency
Fleet Information Warfare Center	Defense Intelligence Agency
Army Information Systems Command	National Security Agency
School for Information Warfare Studies	Central Intelligence Agency
Joint Warfighting Center	Department of Commerce
Joint Spectrum Center	Department of State

Figure 1. Some Organizations Involved in Information Warfare²

Although this list seems complicated, it is important to incorporate the tools each agency has developed for both the defensive and offensive aspects of Information Warfare.

A practical example may help illustrate the importance of this diverse participation. Suppose one of these agencies has discovered a weakness in a particular software and is planning to use this weakness for gathering intelligence information for other national objectives. If the operational commander exploits that same weakness to collapse an enemy information system, then that weakness in that software may become publicly known. The agency then loses its opportunity to continue gathering intelligence when its target realizes their vulnerability. The operational

organization must draw together all these resources to coordinate planning and prevent these types of conflict, making it inherently an inter-agency organization.

National Command Authorities Approval. In a similar vein, Information Warfare may have repercussions far outside the CINC's or even the Department of Defense's normal purview.

Approval for Information Warfare operations will have to come from the National Command Authorities and be coordinated with all the other instruments of national power. As seen in the previous example, some capabilities may be used only once before an adversary realizes they are vulnerable and eliminates the vulnerability. If that capability was needed at a later time, it is lost. Likewise, some Information Warfare actions may have an impact across an adversary's entire economy. As set of authors suggest,

Disrupting an adversary's economy will directly affect the ability of the system to support its military forces, provide the nation's organic essentials (energy, food, minerals and other commodities) and infrastructure (highways, ports, [sic] railroads).³

Also, a virus implanted in a computer in one country can also migrate across national boundaries and infect similar computers worldwide, infecting allies and enemies alike. Similarly, a capability to open "trap doors" in software or hardware may be created secretly and marketed in peacetime. When this capability becomes public, that particular software or hardware may lose its marketability with an adverse impact. The National Security Agency has had just such a problem promoting the "Clipper" data encryption chip since it is widely believed to have a "trap door" that allows law enforcement agencies to break the encryption easily⁴. For these reasons, Information Warfare operations need approval at the national level.

Long-Term Studies. As a third criteria, to conduct Information Warfare will require very fine grained information about an adversary's capabilities. This information requires extensive study by intelligence resources in peacetime. If the particular attack to be used in war is the installation of a virus into an adversary's air defense system, then the type of computer in use, the operating system

employed, network connections within the system, and many other questions need answering before a commander can assess the likelihood of the operation's success. This assessment is crucial to the decision to use Information Warfare versus other warfare methods, such as physical destruction. Therefore, the operational organization must be able to task studies in peacetime and access this detailed information during war.

A good example of how detailed such information ought to be can be found in Command and Control: Support Systems in the Gulf War, by M. A. Rice and A. J. Sammes. The purpose of the book was to gather lessons learned in building British command and control computer systems for deployment in war. But this book also provides a brief overview of the seven principal information systems, nine major software packages operating on at least three different computers used to provide theater connections for the British ground forces in Operation Granby (the British participation in Operation Desert Shield/Desert Storm).⁵ To be useful for targeting a virus, it would also be necessary to know the communication protocols for each software package, how software interrupts are handled in each computer using each software package, and where each system connects user computers into communication nodes. MGen John F. Stewart, Jr., Commander of the US Army Intelligence Center, points out the need for detailed intelligence support for Information Warfare:

The capability to conduct a detailed analysis of the [adversary information systems] will require new research and development of analytical tools as well as the data base structure to support the increased requirements for technical information...⁶

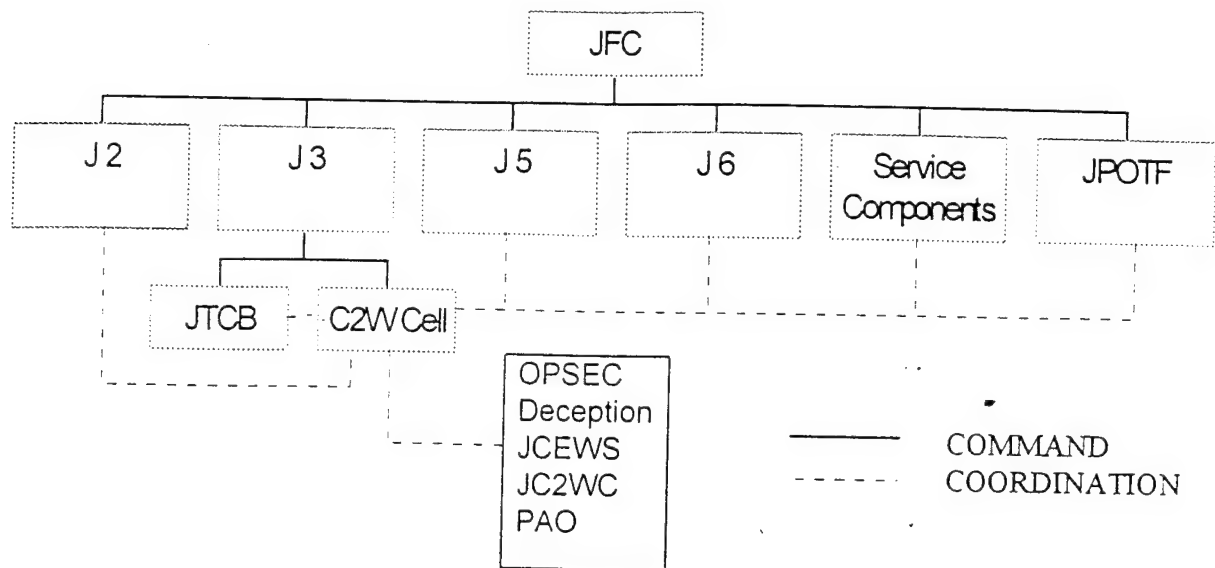
This depth of study must take place continuously, in peacetime as well as during war, and cover a large number of possible adversaries. Therefore, operational units must task long-term, detailed studies during peacetime and have rapid access to the accumulated information during war to effectively use Information Warfare.

THREE MODELS

With the three criteria established to judge the adequacy of a proposed organization, it is time to examine some possible models based on current examples. These models should cover the range of organizational tools commanders are currently using for planning at the operational level. Planning cells represent one way commanders combine staff skills to plan and coordinate operations. The C2W cell is one of many examples of effective planning cells. In addition to planning cells, task forces are often organized to plan and coordinate operations. An excellent example of such a task force is the JPOTF. A final organization commanders use for planning is the component. Although the commander may also have components for Air, Land, and Maritime, the SOC provides an excellent example to explore in seeking an operational proponent for Information Warfare.

C2W Cell Model. The first model to consider is the planning cell. This cell is typically formed under the commander's staff. One example of such a planning cell is the C2W cell composed as shown in Figure 2.

By integrating various representatives from other staff functions, service components, functional components, and other planning cells as well as experts from joint centers outside the theater, the C2W cell focuses many talents on this aspect of warfare and integrates its plans with those other functions. The C2W cell draws upon various service specialties and joint organizations for people. The Joint Center for Electronic Warfare Studies (JCEWS) and Joint Command and Control Warfare Center (JC2WC) provide expertise to support commanders in the field. In addition, coordination with other staff functions is provided by targeting representatives from the Joint Targeting Control Board (JTCB), the JPOTF, the Public Affairs Office (PAO), the Operations Security (OPSEC) Program Office, the intelligence staff (J 2), plans staff (J 5), and the communications and computers staff (J 6). The service components also provide representatives, ensuring full coordination with all the other



C2W Model
Figure 2.⁷

aspects of the operations. These cells usually are built for a specific purpose and are not maintained as operating entities in peacetime.

It is possible to expand the representation for a hypothetical Information Warfare planning cell to include the wide variety of agencies necessary both inside and outside the Department of Defense. In this way, all the various talents needed could be brought together in this model. It would require each agency to be ready to deploy Information Warfare support teams on short notice to form these temporary cells. Many agencies are not currently manned in this way but could adapt to this requirement. How this cell's plans are approved, though, presents somewhat deeper problems.

Approval for C2W operations comes through the normal approval process for all of the commander's operations. Planning is forwarded for coordination and approval by the National Command Authorities. Typically, the C2W plan is contained within plans or Operational Orders published by the commander. It receives no special attention or coordination in the approval process. Each of the members of the cell provide some coordination, but the commander sets priorities on the

expenditure of resources. Disputes about how a particular weapon should be employed are resolved within the staff.

With the potentially sensitive nature of Information Warfare weapons, as explored earlier, it is apparent the "normal" approval process for these weapons is inadequate. The commander may not have a broad enough perspective to judge when to spend one of the "use only once" capabilities like a software trapdoor. To help relieve this concern, it could be possible for those agencies that develop the weapons to selectively authorize specific Information Warfare weapons for use by the commander and his planning cell. This selective release by the creators of the weapons would only be a partial solution, though. It would be natural for the agency who has poured its resources into making one of these weapons, and has therefore only been able to create a few, to be reluctant to expend them readily. In addition, due to the impact of Information Warfare beyond the battlefield, and perhaps beyond the adversary nation's boundaries, neither the commander or the weapons building agency may have sufficient perspective to judge when to use certain weapons. The only level of vision with sufficient perspective to choose to release or withhold Information Warfare weapons like these would be the National Command Authorities.

The National Command Authorities should have the Information Warfare plan set apart from the other theater plans and approved separately. In this way, all of the implications of the weapons can be understood clearly before their release. In this way, capabilities that ought to be reserved for future use are preserved, and weapons that ought to be expended are made available to the commander. The hypothetical Information Warfare cell does not easily allow for this more complicated planning and approval process. In addition to this shortcoming, the planning cell model also has difficulty tasking the long-term, in-depth studies necessary for Information Warfare.

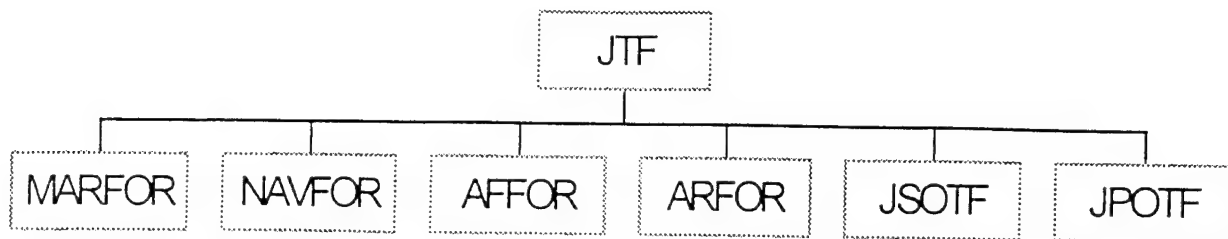
The primary means of peacetime preparation to conduct C2W comes through deliberate planning and identifying essential elements of information for further research by the intelligence staff.

Although this allows the cell to direct information gathering, the essential elements tasking is directed at the key questions the theater commander must answer to execute his operations. The focus of such questions is naturally on a particular adversary's capability, the hard "who, what, when, and where," rather than the softer "why and how" of the adversary's intentions. The adversary's intent and capability both play important roles in how they operate their information systems, and therefore in their vulnerabilities to Information Warfare. Further, the C2W cell typically doesn't exist continuously in peacetime. The lack of continuity may provide too little direction for the long-term studies necessary for Information Warfare.

The information gathering shortcomings of the C2W cell model are not inherent, though, and can be overcome through studies by the agencies that support the commander in building these cells. For example, the JC2WC produces the Proud Flame series of detailed analyses and could achieve the continuity of direction and depth of detail needed for Information Warfare. These agencies would serve as surrogates for the theater commander in directing the necessary studies.

In summary, against the three criteria, the C2W model fits one well and the other two moderately well. The Information Warfare cell could be built of representatives from all the necessary agencies. But, the current approval and coordination process of the planning cell would have to be modified for Information Warfare. Finally, because the cell typically lacks continuity, surrogates would have to direct the studies necessary.

JPOTF Model. A second model to examine is the JPOTF. A recommended structure from Doctrine for Joint Psychological Operations is shown in Figure 3: In this diagram, the JPOTF is coequal with the service components and the Joint Special Operations Task Force (JSOTF). Reporting from the JPOTF goes through the J3, just as the C2W cell did. However, the JPOTF is recommended as a direct member of the JTF staff since the strategic as well as operational importance of Psychological Operations (PSYOP) should be focused at the commander's level.⁹



JPOTF Model
Figure 3.⁸

The composition of the JPOTF is primarily drawn from regionally focused PSYOP battalions.¹⁰ Typically, these task forces are manned by military specialists only. This can result in what Col Jeffrey Jones, and Lt Col Michael Mathews, the Commander and Deputy Commander of the 4th Psychological Operations Group (Airborne) respectively, call “a lack of a multifaceted, coordinated theater information strategy for unified commands to leverage all available information assets.”¹¹ The JPOTF model overcomes some of the lack of representatives from various agencies through a unique approval process requiring coordination with those agencies.¹²

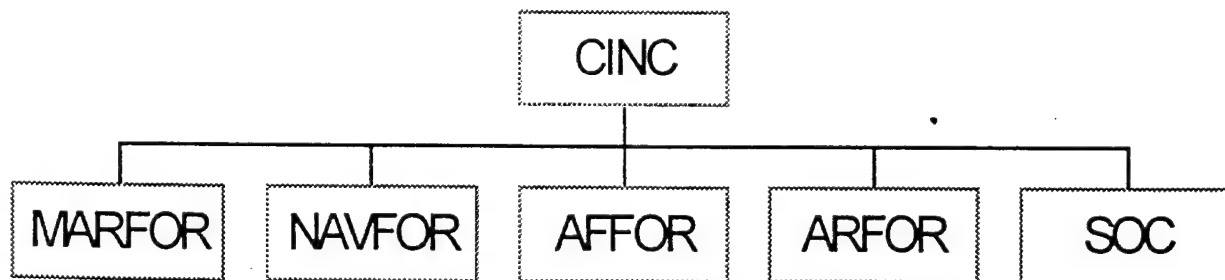
Unlike other operations, PSYOP programs conducted during peace or in conflict are approved by the Under Secretary of Defense for Policy or a designee, the Assistant Secretary of Defense (Special Operations/Low Intensity Conflict). This level of approval provides direct input for plans and programs to be coordinated with the National Security Council and other government agencies.¹³ The strategic impact of tactical and operational PSYOP requires careful consideration and coordination with diplomatic and economic instruments of national power to avoid conflicts and gain maximum benefit from military operations to achieve national objectives. In many ways, the demands for coordination and approval of PSYOP parallel those necessary for Information Warfare.

To provide the necessary intelligence preparation for effective PSYOP, there is also a separate PSYOP Studies Program, managed by Commander, US Special Operations Command

(USCINCSOC), and a separate information system, PSYOP Automated System, supported by the Defense Information Systems Agency.¹⁴ With these tools, commander's staffs and the regionally focused supporting battalions create requests for PSYOP studies in peacetime to focus on particular interests for that commander and can access information generated about potential PSYOP audiences from many agencies. These agencies include the United States Information Agency, the Board for International Broadcasting, the Department of State, and the Drug Enforcement Agency. The studies program provides the kind of depth and broad context detail needed by a hypothetical Information Warfare task force. The plans created for the commanders by the JPOTFs are routed for coordination and approval using the PSYOP Automated System.

In summary, the JPOTF model only moderately fits the inter-agency criteria, but satisfies the need for high-level approval and long-term studies extremely well. The specialized information routing system for PSYOP helps to overcome some of the limitations of a military-only task force. In addition, the regional focus of the units that contribute those military people provides the continuity to create the fine grained information in long-term studies necessary for PSYOP that also would be necessary for Information Warfare.

SOC Model. A third and final model is the integration of Special Operations into CINC and JTF staffs. Joint Publication 3-05.3, Joint Special Operations Operational Procedures, portrays the CINC's organization as shown in Figure 4:



SOC Model
Figure 4.¹⁵

This organization structure has been further strengthened by the recent standardization of the SOC Commander (COMSOC) as a Brigadier General or equivalent within each CINC staff. The COMSOC, also serves as the Joint Forces Special Operations Component Commander and can serve the same function for JTFs directed by the CINC. In addition, since 1987 USCINCSOC has been a force provider to other CINCs and has become in some ways comparable to the services. This elevated status for Special Operations and their forces illustrates the unique nature of Special Operations Forces and their importance to the National Command Authorities. These forces can be employed directly within a theater, or independent from the theater, but with the coordination of the CINC and appropriate State Department members.

Some writers suggest that with the revolution in military or technical affairs evident in Information Warfare, the US should create a new Information Corps. This would provide an elevated status similar to Special Operations. Martin Libicki and James Hazlett advocate such an organization in their article "Do We Need an Information Corps?"¹⁶ These authors cogently point out that making a separate corps inherently segregates Information Warfare from the other forms of warfare and potentially from the other services, as well.

The composition of the SOC is inherently a joint effort by all services, but is primarily a military organization. Despite this nature, the SOC works extensively with a variety of other agencies. Appendix F to Joint Publication 3-05.3, reviews nine different agencies that Special Operations Forces may routinely be involved with.¹⁷ This list includes agencies inside the US government as well as non-governmental organizations. The lack of inter-agency representation within the SOC is overcome by the relationship forged between Special Operations Forces and the Department of State, particularly the Ambassadors and their country teams. This close interaction brings in the detailed knowledge and guidance inherent within the country team to the planning and execution of special operations.

The approval for Special Operations plans, like PSYOP, goes to the Under Secretary of Defense for Policy or a designee, the Assistant Secretary of Defense (Special Operations/Low Intensity Conflict). This level of approval and coordination is also supported by the interaction of the SOC with the Department of State country teams.

Special Operations also require intensive intelligence support. The time sensitive nature of some operations precludes the long-term peacetime study programs such as those for PSYOP. Instead, Special Operations frequently requires very current information, perhaps only minutes or hours old. This up-to-date information requirement is often coupled with a need for extremely detailed information that may only be available through national assets.¹⁸ For the broader, contextual details, Special Operations relies on the Ambassador and the country team to provide the intelligence information.

In summary, the SOC model provides only moderate inter-agency coordination, excellent approval and coordination, but only a limited studies program to support Information Warfare. This model could be improved, however, by providing the interagency representatives and providing a long-term, detailed studies program.

CONCLUSION

These three models represent a range of potential organizations to employ Information Warfare at the operational level. The particular organization chosen depends upon how well each of the three models accomplishes the three criteria described earlier. For a brief review, those functions are 1) interagency participation, 2) approval at National Command Authorities level and coordination with other instruments of national power, and 3) long-term, detailed studies with shared access to information.

All three of the models came close to satisfying the three criteria, but none of the proposed models completely satisfied all the criteria. All three models required augmentation by outside

agencies for development of operations plans. Also, the C2W model did not provide for a separate approval and coordination process necessary to employ Information Warfare weapons. Further, the C2W and SOC models lacked the long-term study system built into the JPOTF model, but C2W used surrogates to continue the detailed studies needed. However, none of the models was completely unsatisfactory. With modifications, any proposed organization could be made workable. The JPOTF model, though, seemed to satisfy the most considerations, especially if augmented by representatives from the various agencies.

Just as many nations wrestled with the difficult question of how to integrate armored vehicles into the operational level of war six decades ago, the United States is trying to wrestle Information Warfare into its operations today. Through a simple framework of three criteria and three models, the readily apparent conclusion is to choose an operational proponent for Information Warfare very similar to the JPOTF. Through an interagency organization, this proponent could formulate plans and integrate them with not only the CINC or JTF staff, but also forward them for approval and coordination with the National Command Authorities and the other instruments of national power. Further, long-term, finely detailed studies of potential adversaries could be carried out in peacetime to aid planners in conducting Information Warfare actions, both in peace and during war. The far-reaching consequences of tactical employment of Information Warfare weapons requires these criteria to thoroughly coordinate the impact of those actions through the operational and strategic levels of war.

Victory smiles upon those who anticipate the changes in the character of war rather than upon those who wait to adapt themselves after the changes have occurred.

Air Marshal Giulio Douhet

ENDNOTES

¹ Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), 7 Feb 96, para 3c, I-3.

² The list of organizations involved in Information Warfare is derived by a review of the "AFCEA Source Book" contained in Signal, Jan 1995, 62-85.

³ H. D. Arnold and others, "Targeting Financial Systems as Centers of Gravity," Defense Analysis, Aug 1994, 181-182.

⁴ Winn Schwartau, Information Warfare, (New York: Thunder's Mouth Press, 1994), 153-155.

⁵ M. A. Rice and A. J. Sammes, Command and control: Support Systems in the Gulf War, (London: Brassey's Ltd, 1994), 28, 54, and 58.

⁶ Mgen John F. Stewart, Jr., "Command and Control Warfare and Intelligence on the Future Digital Battlefield," Army Research, Development and Acquisition Bulletin, Nov-Dec 1994, 15.

⁷ Adapted from "A Nominal C2W Cell," Joint Command and Control Warfare Staff Officer Course, Student Text, Armed Forces Staff College, Jan 1995, p 7-11 and also in Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), 7 Feb 96, Figure IV-1, p IV-3.

⁹ Ibid, para 4b, p III-2.

⁸ Joint Publication 3-53, Doctrine for Joint Psychological Operations, 30 Jul 1993, Figure III-1, p III-5.

¹⁰ Ibid, para 5C(3), p III-4.

¹¹ Col Jeffrey B. Jones and Lt Col Michael P. Mathews, "PSYOP and the Warfighting CINC," Joint Forces Quarterly, Summer 1995, 32.

¹² Joint Publication 3-53, para 10, p IV-7.

¹³ Ibid, para 1b, p II-1.

¹⁴ Ibid, para 1h(10), p II-5 and para 1l, p II-6.

¹⁵ Joint Publication 3-05.3, Joint Special Operations Operational Procedures, 25 Aug 93, Figure III-1, p III-2.

¹⁶ Martin C. Libicki and James A. Hazlett, "Do We Need an Information Corps?", Joint Forces Quarterly, Autumn 1993, 88-97.

¹⁷ Joint Publication 3-05.3, Appendix F, pp F-1 - F-6.

¹⁸ Ibid, para 2, p VI-1.

BIBLIOGRAPHY

- "AFCEA Source Book," Signal, Jan 1995, 62-85.
- Allard, C. Kenneth. "The Future of Command and Control: Toward a Paradigm of Information Warfare," in L. Benjamin Ederington and Michael J. Mazarr, Turning Point: The Gulf War and U.S. Military Strategy. Boulder, Co: Westview Press, 1994.
- Arnold, H. D., et al. "Targeting Financial Systems as Centers of Gravity: 'Low Intensity' to 'No Intensity' Conflict." Defense Analysis, Aug 1994, 181-208.
- Bodnar, John W. "The Military Technical Revolution, from Hardware to Information." Naval War College Review, Summer 1993, 7-21.
- Borchini, Charles P and Mari Borstelmann. "PSYOP in Somalia: The Voice of Hope." Special Warfare, Oct 1994, 2-9.
- Brown, Frederic J. The U.S. Army in Transition II: Landpower in the Information Age. New York, NY: Brassey's (US), Inc., 1993.
- Brungess, James R. Setting the Context: Suppression of Enemy Air Defenses and Joint War Fighting in an Uncertain World. Maxwell Air Force Base, AL: Air University Press, Jun 1994.
- Busey, James B., IV, and Clarence A. Robinson, Jr. "Facing Turbulence, Intelligence Community Revamps Internally." Signal, Apr 1995, 48-51.
- Cerjan, Pual G. And Robert B. Clarke. "NDU Develops a Discipline in Information-Based Warfare." Army, May 1994, 18-19.
- Collins, John M. "Where are Special Operations Forces?" Joint Force Quarterly, Autumn, 1994, 29-31.
- "Commander Pull Intelligence in Information Warfare Strategy." Signal, Aug 1994, 65-68.
- "Dealing With Worms and Viruses." in Thomas W. Madron, Network Security in the '90s, New York, NY: John Wiley & Sons, 1992.
- Evancoe, Paul R. And Mark Bentley. "Computer Viruses Loom as Future Era Weapons." National Defense, Feb 1994, 19-21.
- Franks, Frederick M., Jr. "Winning the Information War." Vital Speeches, 15 May 1994, 453-458.

- Holzer, Robert. "U.S. Navy Begins Information War Effort." Defense News, Aug 29-Sep 4, 1994, 4.
- Jones, Jeffrey B. and Michael P. Mathews. "PSYOP and the Warfighting CINC." Joint Forces Quarterly, Summer 1995, 32.
- Joint Command and Control Warfare Staff Officer Course. Student Text, Armed Forces Staff College, Jan 1995, 7-11.
- Libicki, Martin C. And James A. Hazlett. "Do We need an Information Corps?" Joint Forces Quarterly, Autumn 1993, 88-97.
- Lewonoski, Mark C. "Information War." Essays on Strategy-IX. Washington, DC: National Defense University Press, 1993.
- McKnight, Clarence E., ed. Control of Joint Forces: A New Perspective. Fairfax, Va: Armed Forces Communications and Electronics Association International Press, 1989.
- Rice, M. A. and A. J. Sammes. Command and control: Support Systems in the Gulf War, London: Brassey's Ltd, 1994.
- Rosen, Stephen Peter. Winning the Next War: Innovation and the Modern Military. Ithaca, NY: Cornell University Press, 1991.
- Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.
- Stewart, John F., Jr. "Command and Control Warfare and Intelligence on the Future Digital Battlefield," Army Research, Development and Acquisition Bulletin, Nov-Dec 1994, p 15.
- US Department of Defense, The Chairman of the Joint Chiefs of Staff. Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), 7 Feb 96.
- _____. Joint Publication 3-53, Doctrine for Joint Psychological Operations, 30 Jul 1993.
- _____. Joint Publication 3-05.3, Joint Special Operations Operational Procedures, 25 Aug 93.
- Wriston, Walter B. The Twilight of Sovereignty: How the Information Revolution is Transforming Our World. New York, NY: Scribner's, 1992.